



May 2005

Legislative Audit Division

State of Montana

Report to the Legislature

Information System Audit

Statewide Accounting, Budgeting and Human Resource System (SABHRS)

Department of Administration

This report provides information regarding application controls over SABHRS, and general controls over the related processing environment. It contains six recommendations addressing the ability to overwrite stored data, the presence of PeopleSoft provided user accounts, and access privileges to vendor information, application code, SABHRS development and processing tools, and hardware.

**Direct comments/inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena MT 59620-1705**

**05DP-01
05DP-04**

Help eliminate fraud, waste, and abuse in state government. Call the Fraud Hotline at 1-800-222-4446 statewide or 444-4446 in Helena.

INFORMATION SYSTEM AUDITS

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States Government Accountability Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

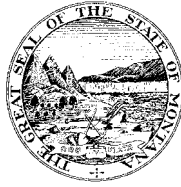
MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Joe Balyeat
Senator John Brueggeman
Senator Jim Elliott
Senator Dan Harrington
Senator Lynda Moss
Senator Corey Stapleton

Representative Dee Brown
Representative Hal Jacobson
Representative Christine Kaufmann
Representative Scott Mendenhall
Representative John Musgrove
Representative Janna Taylor

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel



Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
Tori Hunthausen, IS Audit & Operations
James Gillett, Financial-Compliance Audit

May 2005

The Legislative Audit Committee
of the Montana State Legislature:

This is the report of our information system audit of controls over the Statewide Accounting, Budgeting and Human Resource System. This report contains six recommendations identifying areas where the Department of Administration can strengthen controls by evaluating when the ability to overwrite stored data is necessary, and by addressing access privileges to vendor information, programming code, SABHRS processing tools, and system hardware. In addition, controls can be improved by addressing the need for, and intended use of, delivered user accounts. The department's response to the audit report is contained at the end of the report.

We wish to express our appreciation to the department for their cooperation and assistance.

Respectfully submitted,

(Signature on File)

Scott A. Seacat
Legislative Auditor

Legislative Audit Division

Information System Audit

Statewide Accounting, Budgeting and Human Resource System (SABHRS)

Department of Administration

Members of the audit staff involved in this audit were George Brown and
Jessie Solem.

Table of Contents

Appointed and Administrative Officials	ii
Executive Summary	S-1
Chapter I - Introduction and Background	1
Introduction and Background	1
Audit Objectives	1
Audit Scope and Methodology	1
Prior Audit Recommendation	4
Management Memo	4
Chapter II - Vendor Maintenance.....	5
Vendor Maintenance Introduction	5
Overall Conclusion	5
Unexplained Access to Vendor Information.....	5
Chapter III – Access Security Controls	7
Introduction.....	7
Overall Conclusion	7
Maintaining Historical Data.....	7
Excessive Assignment of “Correct History”	7
Overwriting Vendor History.....	8
Elevated Security Privileges	9
PeopleSoft Provided User accounts	10
Existence of Unused Default User Accounts.....	10
Undocumented Intended Use of a Delivered User Account.....	11
Excessive Access to SABHRS Development and Processing Tools	12
Development Tool Access	12
Processing Tool Access	13
Chapter IV – Physical Security.....	15
Physical Security Introduction.....	15
Overall Conclusion	15
SABHRS Equipment Access	15
Unaccounted for Card Key	15
Unaccounted Use of a Card Key	16
Agency Response.....	A-1
Department of Administration	A-2

Appointed and Administrative Officials

Department of Administration

Janet Kelly, Director

Paul Christofferson, Administrator
Administrative Financial Services Division

Randy Morris, Administrator
State Personnel Division

Jeff Brandt, Acting Chief Information Officer
Information Technology Services Division

SABHRS Service Bureau

Chuck Virag, Bureau Chief

Nyla Johnson
Finance Lead

Jim Sheehy
Information Technology Lead

Theresa Scott
Budget Lead

Martha Watson
Human Resource Lead

Executive Summary

Executive Summary

The Statewide Accounting, Budgeting and Human Resource System (SABHRS) is a commercial software application developed by PeopleSoft and is the state of Montana's system for managing budget development, and financial and human resource information. SABHRS is used by all state agencies to account for and report the use and disposition of all public money and property in accordance with state law. The SABHRS Human Resource Management System (HRMS) and Financial applications were updated to the web-based version 8 in September 2003 and March 2004, respectively.

SABHRS supports the core administrative processes used by all state agencies to account for and record financial and human resource data. The Legislative Audit Division, Information Systems audit team examines selected SABHRS controls and operations each year. The current audit scope is based on specific control testing requested by Legislative Audit Division financial-compliance staff and specific general control testing relating to the environment within which the SABHRS application is developed, maintained, and operated. We performed audit work to meet two objectives: 1) to provide assurance over key SABHRS application controls identified by financial-compliance audit staff, and 2) to evaluate the general controls environment where the SABHRS application resides.

To meet our objectives, we conducted both application and general control testing. General controls represent the foundation for security over SABHRS while application controls are the financial and HRMS controls defined for each business process. Application controls guard the SABHRS Finance and HRMS applications from inadvertent or intentional misuse and ensure data is valid, properly authorized, completely and accurately processed, and available for use. Application controls are divided logically and physically into three separate sub applications: SABHRS Financials, SABHRS Human Resources Management System (HRMS), and the Montana Budget Analysis and Reporting System (MBARS). We did not include MBARS in our audit scope. MBARS is the system used to develop the budget, while the actual financial activity is accounted

Executive Summary

for on the SABHRS Financials system, not MBARS. Through interview, review, and observation, we evaluated whether data and system processing access is controlled, whether processing is controlled to allow valid data to process while capturing invalid data, and whether system payroll tables contain data consistent with state and federal criteria.

General controls represent the controls present in the environment surrounding the application and prevent an individual from bypassing application controls and directly accessing or changing agency data. Through interview and review, we evaluated physical and environmental controls, database and application access security, application change control procedures, and operating system maintenance.

Conclusion

Based on the audit work conducted over the SABHRS application and general controls environment, we identified areas where the Department of Administration can strengthen controls. This report contains six recommendations addressing the ability to overwrite stored data, the presence of PeopleSoft provided user accounts and access privileges to vendor information, application code, SABHRS development and process tools, and hardware.

In addition to this report, we provided a technical memorandum to Legislative Audit staff providing results of key SABHRS application control testing for consideration during financial audits.

Chapter I - Introduction and Background

Introduction and Background

The Statewide Accounting, Budgeting and Human Resource System (SABHRS) is a commercial software application developed by PeopleSoft and is the state of Montana's system for managing budget development, and financial and human resource information. SABHRS is used by all state agencies to account for and report the use and disposition of all public money and property in accordance with state law. The SABHRS Human Resource Management System (HRMS) and Financial applications were updated to the web-based version 8 in September 2003 and March 2004, respectively.

Audit Objectives

SABHRS supports the core administrative processes used by all state agencies to account for and record financial and human resource data. We performed audit work to meet the following objectives:

1. To provide assurances over key SABHRS application controls identified by Legislative Audit Division financial-compliance audit staff. Control objectives were specific to the Finance and HRMS applications. A technical memorandum has been provided to the audit staff for consideration during financial audits.
2. To evaluate the general controls environment where the SABHRS application resides. Control objectives were to provide assurance that controls exist to ensure:
 - ❖ SABHRS application hardware is protected from environmental factors.
 - ❖ Physical access requires user accountability.
 - ❖ The SABHRS application software and data are protected from unauthorized or unnecessary access and modification.
 - ❖ The SABHRS operating systems are current with vendor security updates, and vendor provided configurations are altered.

Audit Scope and Methodology

The audit was conducted in accordance with Government Auditing Standards published by the United States General Accountability Office (GAO). We evaluated the control environment using state law and generally applicable and accepted information technology standards established by the IT Governance Institute.

Chapter I - Introduction and Background

We audit the control environment over SABHRS annually.

SABHRS application controls are divided logically and physically into three separate sub applications: SABHRS Financials, SABHRS HRMS, and the Montana Budget Analysis and Reporting System (MBARS). We did not include MBARS in our audit scope.

MBARS is the system used to develop the budget, while the actual financial activity is accounted for on the SABHRS Financials, not MBARS.

General controls represent the foundation for security over SABHRS, while application controls are the financial and HRMS controls defined for each business process. To meet our objectives, we conducted both general and application control testing. Within the general controls environment, we evaluated physical and environmental controls, database and application access security, application change control procedures, and operating system maintenance. Through interview and review, we tested the general controls environment where the SABHRS application resides. Our testing identified control strengths, as well as controls that can be improved.

▶ Controls identified for improvement

- ❖ Established SABHRS application change control procedures can be circumvented. (Recommendation #3)
- ❖ PeopleSoft provided user accounts were not removed from the SABHRS HRMS database and application. (Recommendation #4)
- ❖ Individuals are improperly allowed anonymous access to SABHRS hardware. (Recommendation #6)

▶ Control strengths

- ❖ Controls exist to ensure SABHRS hardware is protected from environmental factors (i.e., fire, water).
- ❖ A process exists to ensure SABHRS operating systems are current with vendor security updates and vendor provided configurations are modified.
- ❖ Segregation of duties ensures no one individual can provide access authorization to the SABHRS applications and access to SABHRS data.

Chapter I - Introduction and Background

- ❖ Procedures are in place to ensure SABHRS application modifications are working as intended prior to implementation.
- ❖ A process was in place during the Finance application upgrade to ensure the configuration of access privileges provided to users was based on established job responsibilities.
- ❖ SABHRS Services Bureau (SSB) employee's security access to the SABHRS Finance and HRMS applications is authorized.

Application controls operate within the confines of the SABHRS Finance and HRMS applications. These controls guard the application from inadvertent or intentional misuse, and ensure that data is valid, properly authorized, completely and accurately processed, and available for use. Through database table review of access privileges, documentation review, and interview and observation with Department of Administration personnel, we tested key SABHRS human resource and financial application controls. Our testing identified control strengths, as well as controls that can be improved.

▶ Controls identified for improvement

- ❖ Documentation is unavailable to explain why identified agency users have the ability to modify vendor data. (Recommendation #1)
- ❖ Procedures are not in place to prevent unauthorized modifications to vendor information. (Recommendation #1)
- ❖ Security access configuration provides select users the ability to overwrite historical data. (Recommendation #2)
- ❖ Access to SABHRS data processing and development tools is available to users not requiring the access for assigned job duties. (Recommendation #5)

▶ Control strengths

- ❖ Access security controls prevent users from both entering and approving Accounts Receivable transactions.
- ❖ User's access to enter journal transactions is limited to assigned business units.
- ❖ Only authorized users have the ability to issue express check payments and initiate off-cycle payroll processing.

Chapter I - Introduction and Background

- ❖ Procedures exist to ensure state of Montana business rules are protected from unauthorized modifications.
- ❖ Inter-unit journal transactions are approved by the initiating agency before the receiving agency can access the journal.
- ❖ Procedures exist to ensure payroll deduction rates residing in underlying system tables contain rates consistent with the current year governing state and federal requirements.
- ❖ Security access to maintain payroll deduction rates is limited to authorized users.
- ❖ Segregation of duties ensures no one individual can develop and implement automated processes.
- ❖ Controls are in place to ensure users cannot update their own human resource data.
- ❖ Controls exist to identify employees assigned multiple employee identification numbers.
- ❖ Time entry is limited to only valid employees.
- ❖ A process exists to ensure payroll processes within the correct pay period.
- ❖ Procedures exist to ensure processing errors are identified and resolved so data is updated and available to users.
- ❖ A process exists to ensure payroll data posts to the SABHRS Finance application.

Prior Audit Recommendation

The prior audit report on the SABHRS system (04DP-02) included one recommendation to the Department of Administration to revisit the security planning process and update the SABHRS security plan. The department concurred with the recommendation and is actively working on the security plan content. During the audit, we determined the department implemented the recommendation. Because security planning is a dynamic process we will continue to review the security plan in subsequent SABHRS audits.

Management Memo

During the course of our audit, we identified two issues regarding undocumented and outdated procedures, which we believe warrant management's attention. These issues were not included as recommendations in this report, but were discussed with the Department of Administration.

Chapter II - Vendor Maintenance

Vendor Maintenance Introduction

The SABHRS Finance application electronically stores vendor information in the vendor table. The vendor table contains vendor information such as names, addresses, and identification numbers that are referred to during the payment process. Within SABHRS, the process used to add vendors and/or modify vendor information is called vendor maintenance. To protect the integrity of the vendor table, the security access to perform vendor maintenance and make changes to the table is limited. The Administrative Financial Services Division (AFSD) of the Department of Administration is responsible for maintaining vendors associated with the State; however, the division may authorize state agency users access privileges to perform vendor maintenance on vendors associated with their agency. Upon verifying AFSD's approval, vendor maintenance security privileges are granted by the SABHRS Services Bureau (SSB) security personnel.

Overall Conclusion

Based on our vendor maintenance work, we conclude that while AFSD has the ability to delegate vendor maintenance, it has no documented policy on what constitutes a need or when delegation is appropriate. The following section discusses an area where AFSD can improve vendor security.

Unexplained Access to Vendor Information

AFSD may authorize agency users, demonstrating a need, the ability to maintain vendor data associated with their agency directly within SABHRS. While AFSD has the ability to delegate vendor maintenance, a policy does not exist on what constitutes a need or when delegation is appropriate. During our review of the process, we determined AFSD authorized users from Public Employees' Retirement Administration (PERA) and Commissioner of Higher Education (CHE) the ability to perform vendor maintenance. AFSD could not provide documented approval, nor could it explain why individuals from PERA and CHE require the security access. After contacting the agencies, it was explained that PERA uses a subsystem within their agency to provide retiree benefit payments. However, a system limitation within PERA's subsystem prevents

Chapter II - Vendor Maintenance

PERA from issuing benefit payments to retiree's beneficiaries. As a result, PERA uses the vendor maintenance ability within SABHRS to provide beneficiary payments. As of March 2005, AFSD could not explain why CHE has access and requested SSB remove the access.

The vendor maintenance security access granted PERA and CHE users not only allows the agencies to modify their respective vendor information, but also provides access to information on any of the 79,000 vendors associated with the State. AFSD stated it has a verbal agreement with PERA and CHE requiring the users not to modify vendor information associated with the State, only their agency specific vendors. Upon review, we determined a CHE user had unintentionally modified State vendor information on June 3, 2004. AFSD was not aware of the modification. In addition, we identified one PERA user who was granted security access to perform vendor maintenance by SSB without the required AFSD approval. This user's access was used to perform backup responsibilities and was active from March 2004 to May 2004.

The SABHRS Finance application records modifications to vendor information, creating an audit trail. However, AFSD does not utilize the control to monitor vendor changes. AFSD should ensure decisions regarding vendor maintenance activities are documented. To further strengthen controls, AFSD should use monitoring controls provided by SABHRS to ensure vendor access and modifications are authorized.

Recommendation #1

We recommend the Department of Administration:

- A. Establish policy to address security access to the vendor table.**
- B. Evaluate and document PERA and CHE's need to update vendor data and remove unnecessary access.**
- C. Implement monitoring controls to ensure only authorized users have vendor maintenance access and only authorized changes are made to State vendor files.**

Chapter III - Access Security Controls

Introduction

Within the SABHRS application users gain access to data through assigned user accounts and operator roles. Operator roles determine a user's ability to interact with the application by defining what pages a user can access, how information is displayed, and what actions can be applied to the data.

Overall Conclusion

Based on our access security control work, SSB can improve access controls by addressing the ability to overwrite stored data, limiting user access privileges to that which is necessary for the user's job responsibilities, developing procedures to remove PeopleSoft provided user accounts, and documenting the intended use of PeopleSoft provided accounts.

Maintaining Historical Data

SSB and the SABHRS process owners are responsible for configuring and maintaining operator roles. There are three types of actions users can perform to data; update/display, include history and "Correct History."

- ▶ **Update/Display** retrieves only current and future dated rows of data. Users can change future dated rows but not current rows. Users can also add a new current row.
- ▶ **Include History** retrieves all rows of data. However, users can make changes to future dated rows only and add a new current row.
- ▶ **Correct History** retrieves all data rows and allows users to change or correct any row and insert new rows regardless of the effective date.

Excessive Assignment of "Correct History"

"Correct History" allows users to intentionally or unintentionally add, change, or delete historical, current and future data, effectively overwriting information already stored in the database and leaving no audit trail. Without the accountability that is created by an audit trail, there is increased risk that users could make inappropriate changes to data without detection.

Within the SABHRS HRMS application there are approximately 59 operator roles with "Correct History" access capabilities. SSB uses

Chapter III - Access Security Controls

these operator roles to perform certain processes within HRMS. Upon our inquiry, SSB management described the business functions the roles are used to accomplish, but did not explain the required use of “Correct History” to overwrite stored data, as compared to other available access types which retain data history. SSB has not documented instances where “Correct History” is necessary, and as a result, it is unknown whether the ability is required for all 59 roles. We requested SSB management perform a cursory review of the roles to determine if the ability was necessary. Without analyzing each role, SSB management identified three roles improperly configured to provide “Correct History” functionality. SSB recognized the importance of proper role configuration and stated that a regular review of role setup would be implemented to ensure “Correct History” is not unnecessarily available.

Overwriting Vendor History

As discussed in Chapter II, within the Finance application users perform vendor maintenance. There are two operator roles that can be assigned to perform vendor maintenance. Each of these two roles includes the action type “Correct History,” increasing the risk that users could make inappropriate changes to vendor data without detection.

The Finance system provides the functionality to maintain vendor data and maintain historical data. However, as a matter of convenience, AFSD is using “Correct History” capabilities to maintain vendors, including removing and deleting vendor addresses. During the IRS Form 1099 preparation process, the SSB encountered problems issuing the forms. SSB determined that approximately 70 vendor addresses were removed or deleted from the vendor table, omitting the vendors from the creation of the 1099. This occurred because the address designated as the vendor’s 1099 address was no longer in existence (had been overwritten or deleted). In addition, when SSB was in the testing phase for its data archive process, it was determined that certain vendor location information had been deleted. Without the location information, the system cannot determine where to store the data.

Chapter III - Access Security Controls

Controls should be in place to prevent, detect, and help investigate errors and unusual situations. An audit trail provides a tool for such investigations, and the use of “Correct History” does not provide the trail. The use of “Correct History” was first addressed in our report issued in November 1999 (99DP-02). We recommended the removal or close monitoring of “Correct History” access to production data. Subsequently, the number of users with this access was reduced and a state policy was issued in 2000, addressing the need for SABHRS system internal controls. Included in this policy is a requirement that all entries made in SABHRS using “Correct History” must be supported by independent documentation and/or electronic approval. AFSD documents the use of “Correct History” by maintaining agencies requests for vendor additions and modifications; however, they do not maintain internal documentation for each instance of “Correct History” use. The policy speaks to establishing a system of internal controls. The use of “Correct History” for overwriting and deleting data is a control weakness.

Recommendation #2

We recommend the Department of Administration:

- A. Document the requirement(s) necessitating the access privilege.**
- B. Eliminate access privileges from operator roles where not required.**

Elevated Security Privileges

The PeopleSoft application, as delivered, requires SSB modify or enhance SABHRS functionality to meet the business requirements of the various state agencies. These modifications and enhancements require changing and/or adding to the software programming code.

SSB has established code modification procedures to prevent the implementation of unauthorized programming code changes. Controlled implementation of the procedures depends on defined operator roles. Operator roles are assigned access privileges and users are assigned operator roles based on their job responsibilities.

Chapter III - Access Security Controls

Operator roles providing direct access to programming code have the capability to circumvent SSB established procedures. According to guidelines established in SSB's SABHRS security plan, access to perform programming code changes is assigned to only those individuals responsible for applying system changes.

During our security review, we identified three operator roles that are linked to PeopleSoft delivered access privileges, providing the ability to modify programming code. During the SABHRS Finance upgrade in March 2004, the access privileges for these three roles was not reviewed or modified. As a result, four SSB employees assigned the roles have the ability to directly modify programming code, which is greater access than what is necessary for their assigned job duties. Through review of system changes and change management approval documentation, we determined that SSB employees did not use the access to perform unauthorized programming code modifications. Upon notification, the users' access was removed.

SSB management should construct operator roles to provide users only the access necessary to perform their job.

Recommendation #3

We recommend the Department of Administration ensure access privileges are restricted to those necessary to meet assigned job responsibilities.

PeopleSoft Provided User Accounts

The SABHRS application is delivered with user accounts provided by PeopleSoft, which provide access to data within the system. These accounts, known as delivered or default user accounts, are a standard part of PeopleSoft application installations and have fixed username and password combinations.

Existence of Unused Default Accounts

We reviewed the SABHRS application for the presence of default user accounts and identified 21 accounts existing within the HRMS application. These accounts are not used by SSB; however, because

default user accounts are part of PeopleSoft's standard application installations, they are well known. Knowledge of default account information creates opportunities to gain unauthorized access to the HRMS application and data. Upon our notification, SSB management acknowledged the control weakness and stated the accounts would be removed or disabled from use.

According to SSB management, PeopleSoft periodically provides system patches or updates to address identified system problems or to add enhanced functionality. The application of maintenance patches and updates resulted in the re-creation of the default accounts. Although SSB has implemented procedures to remove unused delivered accounts during a major revision or implementation, SSB has not implemented procedures to remove default accounts resulting from installations of maintenance patches or updates.

Undocumented Intended Use of a Delivered User Account

Within the Finance database, SSB's four database administrators use a PeopleSoft delivered user account to implement programming code changes and to identify and resolve application problems. To protect against unauthorized use, SSB modified the password to this account; however, the account username retains its generic default title. Because this account is generically titled with one password, use of the account does not provide for individual accountability to actions performed.

To control use of this account, SSB has adopted an undocumented 'understanding' limiting use of the account to Tuesday nights. This understanding is not a system-enforced limitation and SSB personnel stated that database administrators are authorized to use the account outside Tuesday nights to apply emergency changes (i.e. changes required for successful operation of the application).

We identified 13 instances between August and December 2004 where the generic account was used to modify Finance programming code at times other than Tuesday nights. SSB personnel stated that database administrators do not always remember the Tuesday night limitation

Chapter III - Access Security Controls

and have been reminded of appropriate use of the generic account. Through review of approved system change documentation, we determined all of these changes were appropriate.

State law requires the development and maintenance of written internal policies and procedures to ensure security of data and information technology resources. SSB can strengthen access controls by ensuring maintenance of system software does not jeopardize the security of data and programs stored on the system and by ensuring decisions addressing use of delivered user accounts are documented and monitoring controls are implemented to measure the effectiveness of internal controls.

Recommendation #4

We recommend the Department of Administration:

- A. Establish procedures to review PeopleSoft supplied maintenance patches and updates for default user accounts and remove any unnecessary accounts.**
- B. Document the intended use of the delivered user account and establish procedures to periodically review compliance with the policy.**

Excessive Access to SABHRS Development and Processing Tools

SSB's SABHRS security plan states that agency security officers are responsible for participating in quarterly user access reviews to affirm user access and act on identified exceptions. Although SSB recognizes the importance of access reviews, SSB does not perform periodic review of its employees' access rights to confirm access assigned is appropriate and necessary. During the SABHRS application upgrades, SSB created a process to evaluate SSB employee access to the SABHRS applications. However, as of March 2005, this process has not been implemented.

Development Tool Access

PeopleSoft provides a development tool used to access SABHRS programming code. View only access to the tool is provided to SSB employees with application support responsibilities for problem resolution duties. We identified two SSB employees, who are not developers, with full access. Full access provides the ability to modify

Finance programming code. Access to the development tool was granted to the SSB employees during the Finance application upgrade for security administration and configuration. The two SSB employees have not used their access to the development tool to modify Finance programming code.

Processing Tool Access

SSB is responsible for ensuring that a number of batch processes execute properly each night so that data is updated and available to users in the morning. These programs process all interface transactions provided by agencies, as well as transactions entered online. Daily processes include the loading of transactions, editing, budget checking, journal generating, and posting. The execution of the processes is controlled automatically by a software product called Control-M. Control-M starts processes, checks for successful completion, and notifies the operator when a process fails.

Within Control-M there are two access types: full or view access.

- ▶ Full access is the ability to add to the batch process job stream, view, start and stop jobs and is provided to SSB staff members with application support responsibilities and Department of Administration personnel responsible for monitoring successful completion of nightly batch processing.
- ▶ View access is the ability to view job information only and is provided to Department of Administration personnel responsible for tasks dependant on successful completion of batch processes.

We identified seven SSB employees with full access to Control-M who are not responsible for batch process monitoring or application support.

SSB management stated that three of these individuals do not require access to Control-M and security access was provided to them at one time to accomplish a specific task and their access was not removed when the task was completed. The remaining four SSB employees have full access; however, they only require view access to perform support duties for on-call staff responsible for ensuring successful nightly batch processing. Upon our notification, SSB management requested the access be removed for three of the employees and

Chapter III - Access Security Controls

changed from full to view access for the remaining four employees. Management stated that review of Control-M security access will become part of SSB's established access review process.

SSB management should have a process in place to review and confirm access rights periodically. Periodic review of access rights will ensure users assigned access to SSB's development and processing tools is limited to those individuals requiring the access to perform assigned job duties.

Recommendation #5

We recommend the Department of Administration establish a process and timeline to:

- A. Periodically review SSB employee's access to development and processing tools.**
- B. Ensure privileges are assigned as needed to perform job duties.**

Chapter IV - Physical Security

Physical Security Introduction

Physical security ensures controls are in place to physically protect the facility where the SABHRS equipment resides. Physical security involves restricting physical access to computer resources by limiting access to the building and rooms where they are housed. Physical security controls protect computer resources from intentional or unintentional loss or impairment.

Overall Conclusion

Based on our work, controls exist to ensure SABHRS hardware is safeguarded. The following section discusses areas where physical access to the SABHRS equipment can be improved.

SABHRS Equipment Access

SABHRS equipment is located in the Information Technology Services Division's (ITSD) secured data center. The secured data center has card key access control installed in the form of magnetic security doors and physical access is limited to card key holders. The Office of Cyber Protection (OCP) is responsible for centrally administering access through the security doors. Entry to the secured data center is recorded by an automated system and the OCP reviews recorded entry attempts daily for anomalies (i.e. doors forced open or multiple denials of entry).

Unaccounted for Card Key

The OCP maintains and issues generically named card keys to individuals requiring temporary access to the secured data center. Generically titled cards can be used by anyone in possession of the card and accountability is not maintained for actions performed by the individual. We reviewed a report of card keys used to gain access to data center and identified five generically titled cards providing physical access to the SABHRS equipment. The cards are titled Respond, Desktop Support, Database, "Vendor Name," and Operators. OCP is responsible for securing these cards; however, OCP could not identify the location of one of the generic card keys "Vendor Name."

We reviewed a report of the card keys' use and determined the "Vendor Name" card was used four times in January 2004 to access the secured data center. The secured data center is divided into eight secure areas, each requiring proper card key access to gain physical

Chapter IV – Physical Security

access. The “Vendor Name” card is authorized access to six secured areas, including the area housing SABHRS equipment. The “Vendor Name” card was not used in January to gain entry to the room housing SABHRS hardware; however, the card provides the capability to access SABHRS equipment to the individual in possession. OCP personnel were not aware of the card’s existence and were unable to correlate the card’s use to a documented instance of a specific individual using the card key. Upon our identification of the card, OCP removed the card’s access, disabling it from use.

Unaccounted Use of a Card Key

Mainframe operators are scheduled for around-the-clock duties. On occasion employees may forget their access cards and OCP personnel are not on duty to issue a temporary card key. For these occasions, the OCP has issued the supervisor a card key assigned the name ‘Operators.’

The ‘Operators’ card does not provide for individual accountability to actions performed while in the secured data center. To ensure individual accountability, ITSD has documented procedures for the card’s use, requiring the relieved operator to issue the card by documenting the card’s issuance in a log maintained by the operator’s supervisor.

We reviewed use of the ‘Operators’ card key to ensure compliance with ITSD’s established procedures and to ensure individual accountability was recorded. The ‘Operators’ card has been used eight times since August 2004. Through review of the operator supervisor’s log we determined three of the eight instances of this card’s use could not be associated with a user’s name. According to the operation’s supervisor, the employees issuing the card forgot to log the card’s issuance. The operation’s supervisor was able to identify the card key’s user through employee interview. Upon notification to the OCP of the ‘Operators’ card’s use, OCP disabled the card key due to lack of recorded individual accountability.

The OCP performs daily monitoring of entry attempts to ITSD’s secured data center. However, monitoring activities do not ensure

the ‘Operators’ card key is used as intended, or that all generic cards and locations are known. As custodian of the card keys, OCP should ensure the integrity of all cards used for authentication and implement monitoring controls to ensure generic card keys are known, secured, and used as intended.

Recommendation #6

We recommend the Department of Administration implement monitoring controls to ensure generic card keys are known, secured, and used as intended.

Agency Response

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE



BRIAN SCHWEITZER, GOVERNOR

MITCHELL BUILDING

STATE OF MONTANA

(406) 444-2032
FAX 444-2812

PO BOX 200101
HELENA, MONTANA 59620-0101

May 25, 2005

Scott A. Seacat, Legislative Auditor
Legislative Audit Division
PO Box 201705
State Capitol
Helena, Montana 59620-1705

RECEIVED

MAY 25 2005

LEGISLATIVE AUDIT DIV.

Dear Mr. Seacat:

We have reviewed the November 2003 Statewide Accounting, Budgeting and Human Resource System (SABHRS) Audit Report and the recommendations contained therein. Our response to the recommendations follows.

RECOMMENDATION #1:

We recommend the Department of Administration:

- A. Establish policy to address security access to the vendor table.
- B. Evaluate and document PERA and CHE's need to update vendor data and remove unnecessary access.
- C. Implement monitoring controls to ensure only authorized users have vendor maintenance access and only authorized changes are made to State vendors files.

Response:

- A. We concur. Administrative Financial Services Division (AFSD) staff has reviewed and evaluated the access provided to the State vendor table. AFSD staff will review future requests for access to the vendor table on a case-by-case basis.
- B. We concur. AFSD staff determined that CHE's access to the State vendor table is unnecessary. CHE access was removed. AFSD staff determined that PERA has a valid need and thus access was not changed. This review and evaluation are documented.
- C. We concur. Changes to the State vendor system will be monitored and reviewed periodically by AFSD staff to ensure proper authorization.

RECOMMENDATION #2:

We recommend the Department of Administration:

- A. Document the requirement(s) necessitating the access privilege.
- B. Eliminate access privileges from operator roles where not required.

Response:

- A. We concur. As of March 4, 2005, staff in the SABHRS Services Bureau completed an evaluation of the 59 roles in the Human Resources application with correction capabilities. Based upon this evaluation, correction capability was removed from three roles. Staff is in the process of documenting why the other 56 roles require this access privilege. We will complete the preparation of this documentation by July 1, 2005.
- B. We concur. We will remove access to correction privileges from any roles not requiring this capability.

RECOMMENDATION #3:

We recommend the Department of Administration ensure access privileges are restricted to those necessary to meet assigned job responsibilities.

Response:

We concur. During the Financials upgrade project the four employees cited in the report performed tasks that required the ability to change security objects, which are a form of programming code. We failed to remove this privilege when these individuals no longer required it. The SABHRS Services Bureau has implemented a procedure requiring a Bureau Manager and the Bureau Chief to approve individual staff access privileges. In addition, the Bureau will implement by July 1, 2005 a procedure involving the periodic review of staff access privileges by Bureau managers.

RECOMMENDATION #4:

We recommend the Department of Administration:

- A. Establish procedures to review PeopleSoft supplied maintenance patches and updates for default user accounts and remove any unnecessary accounts.
- B. Document the intended use of the delivered user account and establish procedures to periodically review compliance with the policy.

Response:

- A. We concur. SABHRS Services Bureau staff deactivated all default accounts that are unnecessary. We will document and implement procedures by July 1, 2005 that ensure default accounts provided by PeopleSoft maintenance patches and updates are identified, reviewed, and deactivated when appropriate.
- B. We concur. Staff in the SABHRS Services Bureau will develop a policy describing the appropriate use of delivered user accounts, and establish procedures for monitoring policy compliance by July 1, 2005.

RECOMMENDATION #5:

We recommend the Department of Administration establish a process and timeline to:

- A. Periodically review SSB employees' access to development and processing tools.
- B. Ensure privileges are assigned as needed to perform job duties.

Response:

- A. We concur. The SABHRS Services Bureau will implement by July 1, 2005 a procedure involving the periodic review of staff access privileges by Bureau managers.
- B. We concur. The SABHRS Services Bureau has implemented a procedure requiring a Bureau Manager and the Bureau Chief to approve individual staff access privileges.

RECOMMENDATION #6:

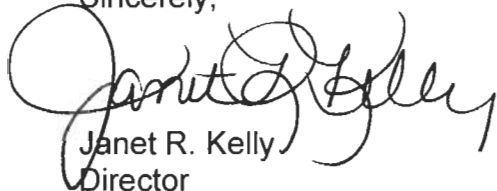
We recommend the Department of Administration implement monitoring controls to ensure generic card keys are known, secured, and used as intended.

Response:

We concur. Over the past year, additional staff has been added to the Office of Cyber Protection (OCP) with the intention of providing additional resources to monitor physical access to the Information Technology Services Division's (ITSD) secured facilities. Due to staff turnover during the past six months, adequate focus has not been provided in this area. As of May 16, 2005, OCP is now fully staffed and intends to provide the resources necessary to ensure that generic card keys are known, secured and used as intended. Two of the cards noted in the audit have been removed from the system and will no longer be used; and we will update our procedures by July 1, 2005 to reflect the use of card keys to access ITSD's secured facilities.

We thank you and your staff for conducting the audit in a professional manner.

Sincerely,



Janet R. Kelly
Director

c: Jeff Brandt